ENCLOSURE (E)

INFORMATION SYSTEMS SECURITY INCIDENT REPORT

June 1998

U. S. Department of Energy
Information Systems Security Incident Report

I. Date/time/and place (site) of incident: _____
Person completing this report_____ Report Date _____
Telephone Number:_____ e-mail _____

II. Type of incident:

☐ Intrusion attempt (successful) ☐ Intrusion attempt (not successful)
☐ Malicious code (virus, trojan horse, etc.) ☐ Unauthorized disclosure of info
☐ Denial of service attack ☐ Misuse
☐ Other: _____

III. Loss associated with the incident:

Time: ☐ < 1 hour ☐ 1-24 hours ☐ 24-48 hours ☐ 2-5 days ☐ > 5 days
Cost: ☐ < $10,000 ☐ $10,000 - $50,000 ☐ > $50,000
☐ Loss, or potential loss, of reputation

IV. Ranking of incident:

☐ Significant ☐ Important ☐ Routine

Justification for ranking_____
_____

Was this incident reportable under ORPS? ☐ Yes ☐ No

V. Classification/sensitivity levels of system/information involved. Check all that apply:

System:

☐ Unclassified

☐ Non-sensitive ☐ Sensitive

☐ Classified

☐ Confidential ☐ NSI (National Security Information)
☐ Secret ☐ FRD (Formerly Restricted Data)
☐ Top Secret ☐ RD (Restricted Data)
☐ SCI (Sensitive Compartmented Information)

U. S. Department of Energy
Information Systems Security Incident Report
Instructions

All incident reports will be reported at an unclassified level. Ensure proper ADC review prior to release.

Incidents will normally be reported once. An exception to this will be the case in which a follow-up report would be submitted if the Incident Ranking changes after the initial report submission.

Submit the report to the CPPM/CSSM [John E. Staley, HR-43, 3-4566] as soon as practical.

Explanation aids in completing the form:

Items I., II., and III. are self explanatory.

Item IV. Use the following guideline when ranking the incident:

Significant - Such as:
- Complete penetration of a system.
- Penetration of a system that exposes a security vulnerability in hardware or software that may be exploited to gain access into other sites within DOE.
- Physical loss sufficient to cause mission or programmatic impact.
- Known loss or compromise of classified or controlled data.
- Use of a system in support of a criminal activity.
- Incident may result in embarrassment to the DOE.
- Cost is greater than $50,000 (Direct cost in equipment or manpower expended in incident recovery)
- Indirect Cost greater than $100,000 (Loss of data, indirect manpower costs).

Important - Such as:
- Loss or compromise of one or more authentication mechanisms that results in suspected compromise of classified or controlled data.
- Penetration of a system that does not allow control of the system or access to all of the data.
- Major misuse of a system by an authorized user (i.e. running a personal business)
- Suspected loss or compromise of classified or controlled data or security software features.
- Incident may result in embarrassment to the site.
- Direct Cost is between $10,000 and $50,000.
- Indirect Costs between $50,000 and $100,000. (Includes loss of data and indirect labor costs)

Routine - Such as:
- External attempt to access a system.
- Minor abuse of a system by an authorized user.
- Direct Cost is less than $10,000 or Indirect cost is less than $50,000.

Item V. is self explanatory.

In item VI. identify the hardware and operating system.

Items VII., VIII., IX., X., XI., XII., and XIII. are self explanatory.

Data/Information:

☐ Unclassified

☐ Non-sensitive
☐ Sensitive

☐ UCNI ☐ NNPI ☐ EXPORT/IMPORT
☐ OUO ☐ CRADA ☐ Business Proprietary
☐ Medical ☐ Personnel ☐ Financial
☐ Proprietary software ☐ Password file(s)
☐ Other _____

☐ Classified

☐ Confidential ☐ NSI (National Security Information)
☐ Secret ☐ FRD (Formerly Restricted Data)
☐ Top Secret ☐ RD (Restricted Data)
☐ SCI (Sensitive Compartmented Information)

VI. What system platform was involved?_____

VII. What was the damage to the affected data?

☐ Stolen ☐ Modified ☐ Deleted ☐ Encrypted ☐ Copied
☐ None ☐ Unknown ☐ Other:_____

VIII. What was the damage to the affected network(s)?

☐ Local access interrupted ☐ Internet access interrupted ☐ None
☐ Other: _____

IX. What was the damage to the affected system?

☐ Service Interrupted:

☐ User Access ☐ E-mail server ☐ Web-server
☐ Ftp ☐ Other: _____

☐ Other: _____

X. How was the incident discovered?

☐ A user ☐ An incident response team ☐ Contacted by another site
☐ Audit logs ☐ Noticed unusual activity/behavior ☐ Anti-virus software
☐ Other: _____

XI. Was the originating source of the incident located? ☐ Yes ☐ No

If yes, what was the source of the incident?

1. For malicious code:

   ☐ Diskette ☐ Downloaded file ☐ Attachment
   ☐ Obtained while on foreign travel

2. For an intrusion attempt:

   ☐ Insider
   ☐ Outsider

      ☐ .gov ☐ .mil ☐ .edu ☐ .org ☐ .com ☐ .net ☐ Other_____

   ☐ Non-US. If Non-US what country: _____

3. For a denial-of-service attack:

   ☐ Insider
   ☐ Outsider

      ☐ .gov ☐ .mil ☐ .edu ☐ .org ☐ .com ☐ .net ☐ Other_____

   ☐ Non-US. If Non-US what country: _____

XII. Was law enforcement contacted regarding this incident? ☐ Yes ☐ No

If Yes: Was the IG contacted regarding this incident? ☐ Yes ☐ No

XIII. Was CIAC contacted regarding this incident? ☐ Yes ☐ No

If yes: CIAC incident number: _____

Date incident opened: _____ Date incident closed: _____